

**UNITED STATES DEPARTMENT OF COMMERCE****Patent and Trademark Office**Address: COMMISSIONER OF PATENTS AND TRADEMARKS  
Washington, D.C. 20231

(HO)

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.
-----------------	-------------	----------------------	---------------------

08/949,525 10/14/97 WIENER

M ENT970827-1

LM02/0601

**EXAMINER**

MEISLAHN, D

**ART UNIT**

2767

**PAPER NUMBER**

14

DATE MAILED: 06/01/00

Please find below and/or attached an Office communication concerning this application or proceeding.

**Commissioner of Patents and Trademarks**

## Office Action Summary

Application No. <b>08/949,525</b>	Applicant(s) <b>Michael J. Wiener And Josanne M. Otway</b>
Examiner <b>Douglas Melslahn</b>	Group Art Unit <b>2767</b>

Responsive to communication(s) filed on May 11, 2000

This action is FINAL.

Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under Ex parte Quayle 1035 C.D. 11; 453 O.G. 213.

A shortened statutory period for response to this action is set to expire 3 month(s), or thirty days, whichever is longer, from the mailing date of this communication. Failure to respond within the period for response will cause the application to become abandoned. (35 U.S.C. § 133). Extensions of time may be obtained under the provisions of 37 CFR 1.136(a).

### Disposition of Claim

- Claim(s) 1-26 is/are pending in the application.  
Of the above, claim(s) \_\_\_\_\_ is/are withdrawn from consideration.
- Claim(s) \_\_\_\_\_ is/are allowed.
- Claim(s) 1-26 is/are rejected.
- Claim(s) \_\_\_\_\_ is/are objected to.
- Claims \_\_\_\_\_ are subject to restriction or election requirement.

### Application Papers

- See the attached Notice of Draftsperson's Patent Drawing Review, PTO-948.
- The drawing(s) filed on \_\_\_\_\_ is/are objected to by the Examiner.
- The proposed drawing correction, filed on \_\_\_\_\_ is  approved  disapproved.
- The specification is objected to by the Examiner.
- The oath or declaration is objected to by the Examiner.

### Priority under 35 U.S.C. § 119

- Acknowledgement is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d).
- All  Some\*  None of the CERTIFIED copies of the priority documents have been
- received.
- received in Application No. (Series Code/Serial Number) \_\_\_\_\_.
- received in this national stage application from the International Bureau (PCT Rule 17.2(a)).

\*Certified copies not received: \_\_\_\_\_

- Acknowledgement is made of a claim for domestic priority under 35 U.S.C. § 119(e).

### Attachment(s)

- Notice of References Cited, PTO-892
- Information Disclosure Statement(s), PTO-1449, Paper No(s). \_\_\_\_\_
- Interview Summary, PTO-413
- Notice of Draftsperson's Patent Drawing Review, PTO-948
- Notice of Informal Patent Application, PTO-152

-- SEE OFFICE ACTION ON THE FOLLOWING PAGES --

## **DETAILED ACTION**

### ***Response to Request for Reconsideration***

1. This action is in response to the after-final request for reconsideration filed 11 May 2000.
2. Applicant's request for reconsideration of the finality of the rejection of the last Office action is persuasive and, therefore, the finality of that action is withdrawn. Applicant's arguments were persuasive.

### ***Response to Arguments***

3. Applicant's arguments with respect to claims 1-26 have been considered but are moot in view of the new ground(s) of rejection.

### ***Claim Rejections - 35 USC § 103***

4. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

5. Claims 1-4, 6, 8-18, 20-24, and 26 are rejected under 35 U.S.C. 103(a) as being unpatentable over Lewis (5761306) in view of Ellison (Generalized Certificates).

Lewis shows a public key replacement system. Figure 2 shows that both private and public keys are updated. Lewis' system causes a key switch. Lewis does not say that there are certificates with expiry data that is user selectable. Ellison talks at throughout his disclosure about certificates, which are used to authenticate public keys. These certificates are issued by certificates are issued by certification authorities. On

Art Unit: 2767

page five, Ellison says that he believes that there is a problem with CRLs. He believes, as he says in the paragraph bridging pages five and six, that certificates should each include a validity field. He goes on to say that “[i]t is up to you to decide how long you’re willing to have an invalid certificate out in the world – and to define the validity period accordingly. This is a matter of normal risk management.” An example of decisions made based on risk management is demonstrated by buyers of RSA’s keys; users can get a short-lived key pair for free but have to pay for longer lasting keys. An e-mail message that begins on page seven and ends on page 9 outlines the benefits of eliminating CRLs. Therefore it would have been obvious to a person of ordinary skill in the art at the time the invention was made to give users the ability to define the validity period for certificates, as taught by Ellison, in the public key update system of Lewis.

Additional material in claim 9 is anticipated by Lewis. Claim 2 is shown by Ellison. Claim 3 is met by Lewis in lines 64-65 of column 7. Claim 6 is inherent to Ellison in that an interface to select validity periods is required.

6. Claims 5, 19, and 25 are rejected under 35 U.S.C. 103(a) as being unpatentable over Lewis and Ellison as applied to claims 1, 14, and 21 above, and further in view of applicant’s admitted prior art.

Lewis and Ellison teach the selection of key validity periods on a per client basis. They do not specify a time frame in which a client can request key updates. In lines 14 through 19 of page 2, applicant discusses a conventional public key system in which keys have a fixed default period that is “ . . . generally a fixed percentage or a total key lifetime . . . ” Official notice is taken that fixed length renewal periods are old and well-

known. Therefore it would have been obvious to a person of ordinary skill in the art at the time the invention was made to set key update periods that are based on a fixed number of days and a percentage of a key's lifetime. This method provides flexibility by giving clients who have keys that have either extremely long or extremely short lifetimes two options as to when to update their keys.

7. Claim 7 is rejected under 35 U.S.C. 103(a) as being unpatentable over Lewis and Ellison as applied to claim 1 above.

Lewis and Ellison teach the selection of key validity periods on a per client basis. In their system, keys are created by a user and then sent to a certification authority for a certificate. In another implementation of public-key cryptosystems, the certification authority both generates and verifies the public/private key pair, sometimes on request. The previously mentioned RSA key marketing method exemplifies this. Therefore it would have been obvious to a person of ordinary skill in the art at the time the invention was made to apply the teachings of Lewis and particularly Ellison to the well-known public key cryptosystem where a certification authority produces the key pair.

### ***Conclusion***

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Douglas J Meislahn whose telephone number is (703) 305-1338. The examiner can normally be reached between 9AM - 6PM, except every other Friday.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Tod Swann can be reached on (703) 308-7791. The fax phone numbers for

Art Unit: 2767

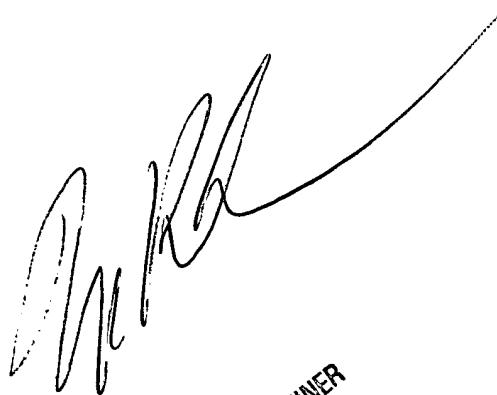
the organization where this application or proceeding is assigned are (703) 308-9051 for regular communications and (703) 308-9052 for After Final communications.

Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the receptionist whose telephone number is (703) 305-3900.

Douglas J Meislahn  
Examiner  
Art Unit 2767

DJM

May 24, 2000



TOD R. SWAGER  
SUPERVISORY PATENT EXAMINER  
GROUP 2700